REMARKS

This Application has been carefully reviewed in light of the Office Action mailed March 17, 2006. Applicants cancel Claim 33 without prejudice or disclaimer. Applicants respectfully request reconsideration and favorable action in this case.

Section 103 Rejections

The Examiner rejects Claims 1-2, 5-7, 10-12, 15-17, 20 and 25-32 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,067,410 issued to Nachenberg ("*Nachenberg*") in view of U.S. Patent Publication No. 2002/01783875 to Whittaker et al. ("*Whittaker*"). Claim 1 recites:

> A method for restoring a computer system modified by malicious code, comprising:
>
> scanning the computer system for the malicious code;
>
> identifying the malicious code;
>
> retrieving from a data file, information relating to the malicious code including at least one command used for restoring the computer system to a state that existed prior to modification by the malicious code; and
>
> executing the at least one command to restore the computer system to the state as the computer system existed prior to modification by the malicious code, wherein the at least one command is used for restoring at least a portion of the computer system other than a host file having the malicious code to the state that existed prior to the portion of the computer system having been modified by the malicious code.

Nachenberg and *Whittaker*, both alone and in combination, fail to disclose, teach, or suggest every element of Claim 1. For example, the proposed *Nachenberg-Whittaker* combination fails to disclose "retrieving from a data file, information relating to the malicious code including at least one command used for restoring the computer system." In addressing this element, the Examiner asserts that:

> Nachenberg is directed to an emulation repair system (ERS)...comprising...retrieving from a data file, information relating to the malicious code including at least one command used for restoring the computer file [system] to a state as the computer file [system] existed prior to modification by the malicious code [Nachenberg teaches a virus definition file (i.e. a data file) comprising an entry or virus definition for each known virus. Each virus definition contains information specific to a virus or a family of such viruses, see col. 7, lines 54-57. That is, the ERS uses the virus type at input as an index to an appropriate virus definition in virus definition file, see col. 7, lines 58-60]

Office Action, p. 3.

To whatever extent this may be true, Applicants respectfully note that the Examiner asserts only that, in the system of *Nachenberg*, "[e]ach virus definition contains information specific to a virus or a family of such viruses[.]" Regardless of whether the virus definitions of *Nachenberg* do "contain[] information specific to a virus or a family of such viruses" as the Examiner contends, Applicants respectfully note that the Examiner does not contend that the data file of *Nachenberg* includes "information relating to the malicious code including at least one command used for restoring the computer system to a state that existed prior to modification by the malicious code" as required by Claim 1.

Moreover, in addressing the "executing the at least one command" element of Claim 1, the Examiner asserts that "[the] *overlay module includes code* (i.e. commands) for locating and co-opting virus repair code to restore host file (i.e. executing at least one command to restore (and curing)) the computer system and/or infected file to the state as it existed prior to modification by the malicious code)" *Office Action*, p. 3, emphasis and underlining added. Thus, to the extent, if any, that *Nachenberg* discloses any "command used for restoring the computer system," such command or commands are stored in the overlay module and not the virus definition file. The virus definition file includes no such commands.

As a result, *Nachenberg* fails to disclose, teach, or suggest "retrieving from a data file, information relating to the malicious code including at least one command used for restoring the computer system." The Examiner is silent as to whether *Whittaker* discloses this element, but *Whittaker* also does not disclose, teach, or suggest this element of Claim. Consequently, the proposed *Nachenberg-Whittaker* combination fails to disclose, teach, or suggest "retrieving from a data file, information relating to the malicious code including at least one command used for restoring the computer system" as recited by Claim 1.

Additionally, the proposed *Nachenberg-Whittaker* combination is improper for at least several reasons. First, Applicants respectfully note that, to establish a prima facie case of obviousness, the Examiner must identify within the references some suggestion or motivation to combine the references. M.P.E.P. § 2143. Applicants respectfully assert that the Examiner provides no such suggestion or motivation. With respect to the proposed *Nachenberg-Whittaker* combination, the Examiner states only that:

> Therefore it would have been obvious to one of ordinary skill in the art to modify the method/system of Nachenberg, to incorporate the protective

> program, taught by Whittaker, because detecting malicious code at the application level (host file as is the case in Nachenberg) does not prevent the possibility of malicious code accessing the operating system and its registry file.
>
> *Office Action*, p. 4.

Thus, the Examiner identifies the absence of certain features in one reference (i.e., that the system of *Nachenberg* does not prevent the possibility of malicious code accessing the operating system and its registry) as the sole motivation for combining the two references. Applicants respectfully note that this reasoning would completely vitiate the requirements for establishing a prima facie case and would allow combination of any possible references. Moreover, these conclusory statements, however, do not identify any motivation or suggestion *within the references* to combine the references as required by M.P.E.P. § 2143 and amount to hindsight reconstruction of Claim 1. Thus, the proposed combination is improper.

Second, Applicants respectfully note that "[a] prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention." *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 U.S.P.Q. 303 (Fed. Cir. 1983), *cert. denied,* 469 U.S. 851 (1984). (M.P.E.P. § 2141.02). Not only does *Nachenberg* not provide any motivation for combining the teachings of *Nachenberg* with the teachings of *Whittaker*, but *Nachenberg* actually teaches away from such a combination. *Nachenberg* notes that:

> In order to accomplish the mischief for which they are designed, software viruses must gain control of a computer's central processing unit (CPU). Viruses *typically* do this by attaching themselves to an executable file (host file) and modifying the executable image of the host file at its entry point to pass control of the CPU to the viral code.
>
> Col. 4, ll. 25-27, emphasis and underlining added.

Thus, instead of motivating the proposed combination as the Examiner contends, *Nachenberg* would teach away from the need for addressing changes to the registry by noting that the typical concerns raised by viruses relate to changes to the host file and not changes to the registry. As a result, *Nachenberg* would discourage one skilled in the art from combining the teachings of *Nachenberg* with those of *Whittaker* to protect against changes to the registry

file. Thus, *Nachenberg* teaches away from the combination, and the combination is thus improper.

As a result, the proposed *Nachenberg-Whittaker* combination fails to disclose, teach, or suggest every element of Claim 1. Additionally, the proposed *Nachenberg-Whittaker* combination is also improper. Claim 1 is thus allowable for at least these reasons. Applicants respectfully request reconsideration and allowance of Claim 1 and its dependents.

Although of differing scope from Claim 1, Claims 6, 11, 16, and 33 include elements that, for reasons substantially similar to those discussed with respect to Claim 1, are not disclosed, taught, or suggested by the proposed *Nachenberg-Whittaker* combination. Additionally, as noted above, the proposed *Nachenberg-Whittaker* combination is improper. Claims 6, 11, 16, and 33 are thus allowable for at least these reasons. Applicants respectfully request reconsideration and allowance of Claims 6, 11, 16, and 33, and their respective dependents.

The Examiner rejects Claims 3, 8, 13 and 18 under 35 U.S.C. § 103(a) as being unpatentable over *Nachenberg* and *Whittaker* in view of U.S. Patent No. 6,401,210 to Templeton ("*Templeton*"). Claims 3, 8, 13, and 18 depend from Claims 1, 6, 11, and 16, respectively, which have all been shown above to be allowable. Claims 3, 8, 13, and 18 are thus allowable for at least these reasons. Applicants respectfully request reconsideration and allowance of Claims 3, 8, 13, and 18.

The Examiner rejects Claims 4, 9, 14, and 19 under 35 U.S.C. § 103(a) as being unpatentable over *Nachenberg* and *Whittaker* in view of a document entitled "Happy99.Worm Removal Tool" ("*FIXHAPPY*"). Claims 4, 9, 14, and 19 depend from Claims 1, 6, 11, and 16, respectively, which have all been shown above to be allowable. Claims 4, 9, 14, and 19 are thus allowable for at least these reasons.

Furthermore, several dependents of Claims 1, 6, 11, and 16 are allowable for additional reasons. As one example, Claim 4 recites:

> The method of claim 1, wherein the malicious code modifies at least one file and said method comprises:
>
> reading from the modified file, a name of a second file; and
>
> modifying the second file.

The proposed *Nachenberg-Whittaker-FIXHAPPY* combination fails to disclose, teach, or suggest every element of Claim 4. For example, the proposed *Nachenberg-Whittaker-*

FIXHAPPY combination fails to disclose "reading from [a] modified file, a name of a second file." As the Examiner concedes, *Nachenberg*, even as modified by *Whittaker*, fails to disclose this additional element of Claim 4. *Office Action*, p. 6. Moreover, the Examiner fails to identify any portion of *FIXHAPPY* that discloses "reading from a modified file, a name of a second file," and *FIXHAPPY* in fact fails to disclose this element of Claim 4. As a result, the proposed *Nachenberg-Whittaker-FIXHAPPY* combination fails to disclose every element of Claim 4.

Additionally, the proposed *Nachenberg-Whittaker-FIXHAPPY* combination is improper. As discussed above with respect to Claim 1, combination of *Nachenberg* and *Whittaker* is improper. In addition, combination of *Nachenberg* with *FIXHAPPY* is also improper. Applicants respectfully remind the Examiner that, to establish a prima facie case of obviousness, the Examiner must identify within the references some suggestion or motivation to combine the references. M.P.E.P. § 2143. Applicants respectfully assert that the Examiner provides no such suggestion or motivation for the proposed *Nachenberg-Whittaker-FIXHAPPY* combination. With respect to the proposed *Nachenberg-Whittaker-FIXHAPPY* combination, the Examiner states only that:

> It would have been obvious to one of ordinary skill in the art to modify Nachenberg's repair system to incorporate the feature taught in Happy99.worm Removal Tool to not only restore the content of infected file(s) (in system directory), but also to modify other file(s) infected (in system registry) to reduce the spread of the worm (virus), especially when a user is online or connected to a network, see the document.
>
> *Office Action*, p. 4.

Thus, the Examiner identifies the self-contained benefits of one reference as the sole motivation for combining the two references. The benefits identified by the Examiner are provided by Applicants *FIXHAPPY* reference *by itself*. They do not in any way motivate any combination with *Nachenberg*. Applicants respectfully note that this reasoning would also completely vitiate the requirements for establishing a prima facie case and would allow combination of any possible references. Moreover, these conclusory statements do not identify any motivation or suggestion within the references *to combine* the references as required by M.P.E.P. § 2143 and amount to hindsight reconstruction of Claim 4. Thus, the proposed combination is improper.

As a result, the proposed *Nachenberg-Whittaker-FIXHAPPY* combination fails to disclose, teach, or suggest at least these additional elements of Claim 4. Although of differing scope from Claim 4, Claims 9, 14, and 19 include elements that, for reasons substantially similar to those discussed with respect to Claim 4, are not disclosed, taught, or suggested by the proposed *Nachenberg-Whittaker-FIXHAPPY* combination. The proposed *Nachenberg-Whittaker-FIXHAPPY* combination is also improper. Claims 4, 9, 14, and 19 are thus allowable for at least these additional reasons. Applicants respectfully request reconsideration and allowance of Claims 4, 9, 14, and 19.

Section 102 Rejections

The Examiner rejects Claim 33 under 35 U.S.C. § 102(e) as being anticipated by *Whittaker*. While Applicants respectfully traverse this rejection, Applicants cancel Claim 33 for the purposes of advancing prosecution. Applicants wish to note that, with respect to all cancellations and amendments herein, Applicants reserve the right to pursue broader subject matter than that already claimed through the filing of continuations and/or other related applications.

Conclusions

Applicants have made an earnest attempt to place this case in condition for allowance. For the foregoing reasons, and for other reasons clearly apparent, Applicants respectfully request full allowance of all pending Claims. If the Examiner feels that a telephone conference or an interview would advance prosecution of this Application in any manner, the undersigned attorney for Applicants stands ready to conduct such a conference at the convenience of the Examiner.

No fees are believed to be due, however, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 02-0384 of Baker Botts L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicants

Todd A. Cason
Reg. No. 54,020

2001 Ross Avenue, Suite 600
Dallas, Texas 75201-2980
(214) 953-6452

Date: 6/15/06

CORRESPONDENCE ADDRESS:

Customer Number: **05073**